Best Practices in Complex Electronic Hardware Development

Terrence L. (Terry) Leier
Mgr-Certification Support; DER

Robert W. (Wayne) Haug
Sr. Product Integrity Engr.

July 28, 2005

Rockwell Collins

Topics

- **History – How We got Here**

- **Currently – Where We Are Now**

- **Best Practices – What We Are Doing Comply**

- **Future – What We Anticipate**

Rockwell Collins

Acronyms

- **CEH – Complex Electronic Hardware, i.e., custom micro-coded components or devices**

- **CIA – Change Impact Analysis (conceptually same as for SW)**

- **HAS – Hardware Accomplishment Summary**

- **PHAC – Plan for Hardware Aspects of Certification**

Rockwell Collins

History - Timeline

- **Early 90's: Tailorable devices became available**

- **Circa '93: Concern that micro-coding in these devices could circumvent design assurance requirements**

- **Circa '95: RTCA launches SC-180; EUROCAE jointly launches WG-46; development of a consensus document begins**

- **Mid-90's – Present: Issue Paper for Programmed Logic Devices**

- **1998-2000: DO-TBD (forever)**

- **April 19, 2000: DO-254/ED-80**

- **April 2000 – June 2005: AC 20-CEH (forever)**

- **June 30, 2005: AC 20-152, which acknowledges and delineates applicability of DO-254**

- **Expected: Order 8150.1c Appendix 1 inclusion of CEH in TSO submittals**

Rockwell Collins
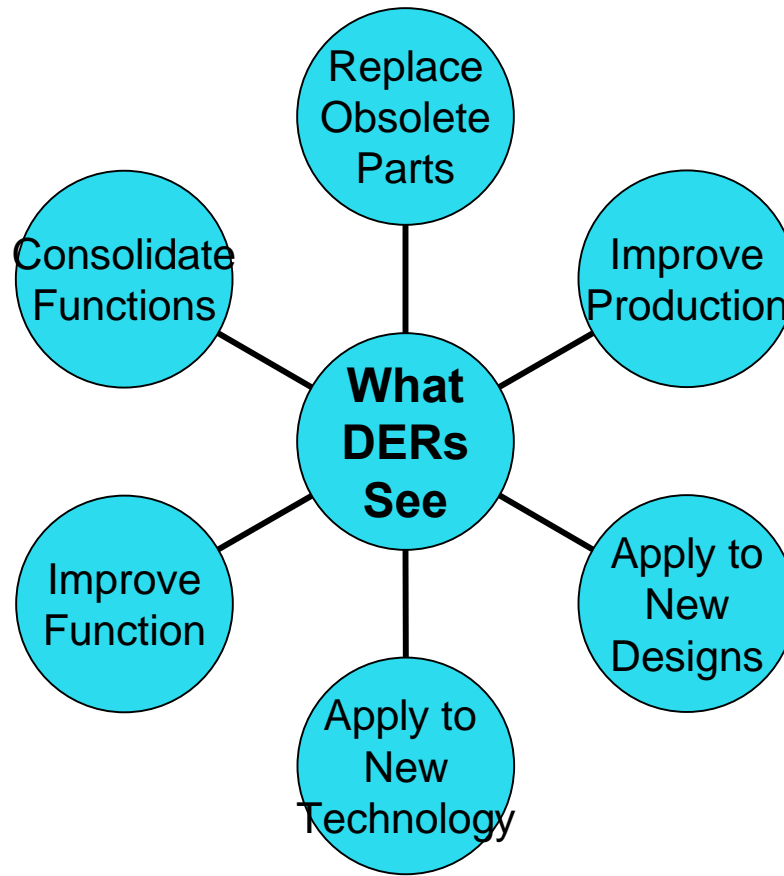
History – Collins Activities

- **1993: Initiated processes for ASIC planning, development and design documentation**

- **1995-2000: Co-chaired and participated in SC-180**

- **Mid-90's – Present:**

  — **Support aircraft program requests for proposed response to CEH issue papers**

  — **Increase expectations for capture of engineering documentation**

  — **Communicate intentions and coordinate expectations with regulatory authorities**

Rockwell Collins
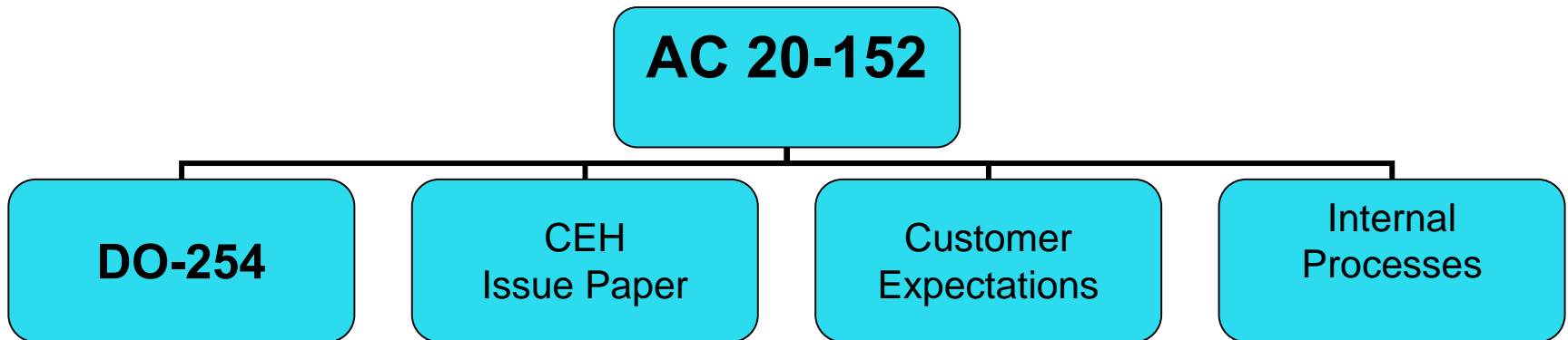
History – Guiding Principle

- ***Documentation of Prudent Engineering***

  — **Originally the FAA was concerned about Prudent Engineering for CEH's**

  — **A 10 year History of successful CEH implementation lead to a more conservative approach to CEH documentation**

  — **No reverse engineering required for fielded products, but expected to include documentation for new development projects**

  — **Now forward: Use guidance of AC 20-152**

Rockwell Collins
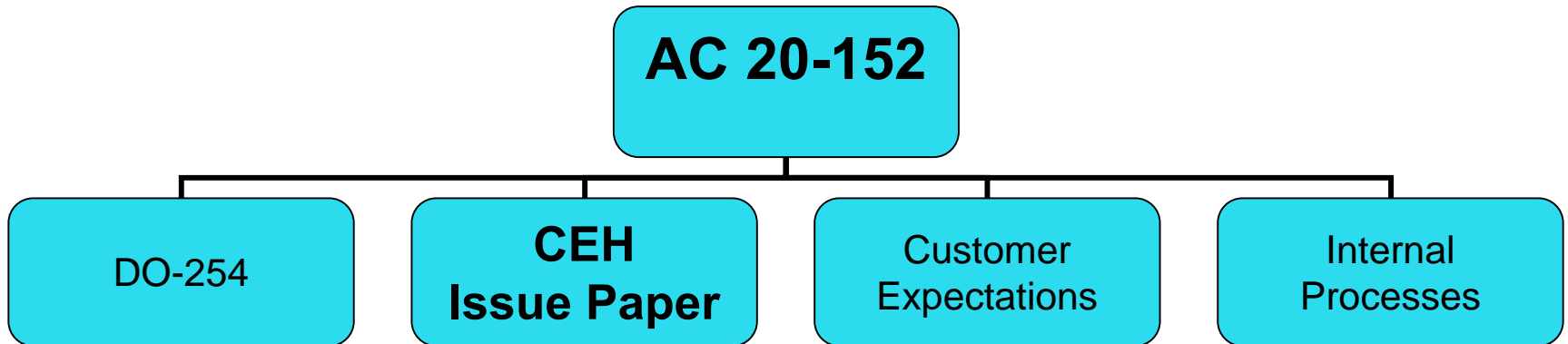
A central circle labeled **What DERs See** connects to six surrounding circles:
- Replace Obsolete Parts
- Improve Production
- Apply to New Designs
- Apply to New Technology
- Improve Function
- Consolidate Functions

Rockwell Collins

```
                    ┌─────────────┐
                    │  AC 20-152  │
                    └──────┬──────┘
        ┌────────────┬─────┴─────┬────────────┐
  ┌─────────┐  ┌──────────┐ ┌──────────┐ ┌──────────┐
  │ DO-254  │  │   CEH    │ │ Customer │ │ Internal │
  │         │  │Issue Paper│ │Expectations│ │Processes │
  └─────────┘  └──────────┘ └──────────┘ └──────────┘
```
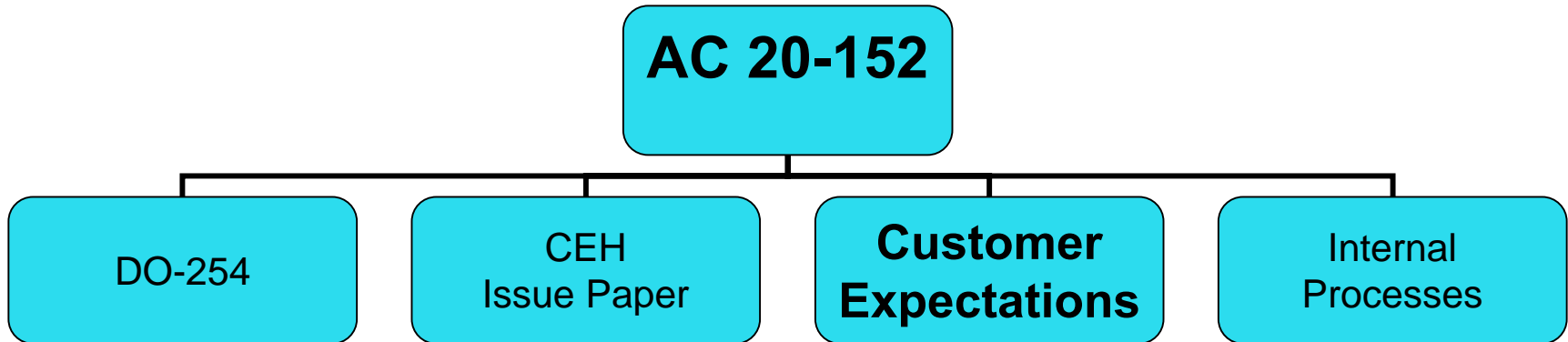
- **In the process of transitioning vernacular:**

  - from "comply with applicable portions of DO-254"

  - to " comply with AC 20-152"

- DO-254 Appendix A matrix is useful (mapping discussed later)

- Anticipate that engineers will use guidance for Level D devices

Rockwell Collins

```
                    ┌──────────────┐
                    │  AC 20-152   │
                    └──────┬───────┘
        ┌──────────────┬───┴───┬──────────────┐
┌───────────┐ ┌──────────────┐ ┌───────────┐ ┌───────────┐
│  DO-254   │ │    CEH       │ │ Customer  │ │ Internal  │
│           │ │ Issue Paper  │ │Expectations│ │ Processes │
└───────────┘ └──────────────┘ └───────────┘ └───────────┘
```
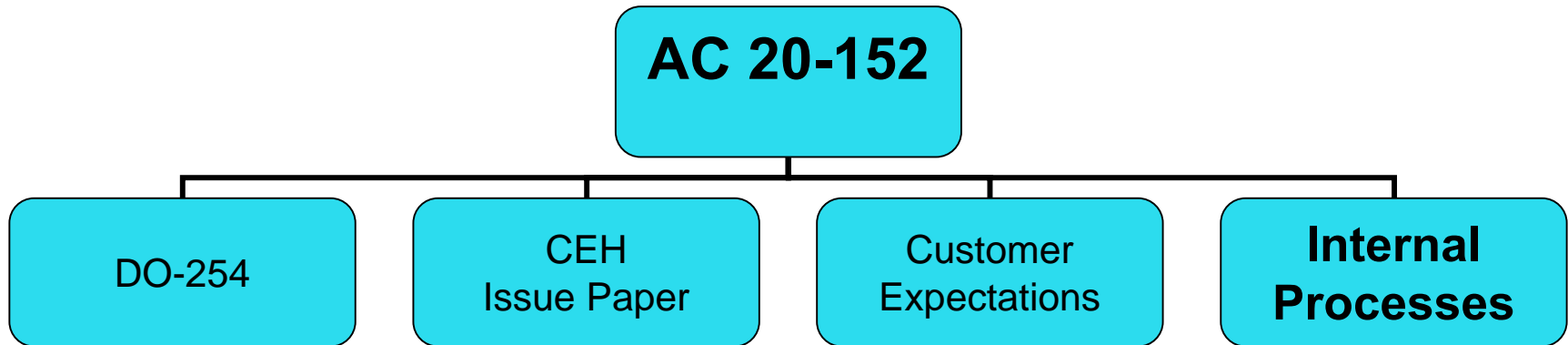
- Note: Applicable to GIP, CRI, or similar document by any other title or form by a regulatory agency

- **Projection for future responses: " comply with AC 20-152"**

- **DER Involvement: Review of Issue Paper to insure appropriate understanding and response**

- Question: Will these go away?

Rockwell Collins

Current State (cont.)

```
                    ┌─────────────┐
                    │  AC 20-152  │
                    └──────┬──────┘
        ┌──────────┬───────┼───────┬──────────┐
┌───────┴───┐ ┌────┴─────┐ ┌──┴────────┐ ┌────┴──────┐
│  DO-254   │ │   CEH    │ │ Customer  │ │ Internal  │
│           │ │Issue Paper│ │Expectations│ │ Processes │
└───────────┘ └──────────┘ └───────────┘ └───────────┘
```

- Large aircraft manufacturers have additional requirements (e.g., Boeing D6-81999; Bombardier in process, others?)

- Program Management and Engineering responsibility to comply

- **DER Involvement: Support discussions with customer, understand nature of additional requirements and evaluate resulting documentation**

Current State (cont.)

```
                    ┌─────────────┐
                    │  AC 20-152  │
                    └──────┬──────┘
          ┌────────┬───────┼───────┬────────┐
    ┌─────┴───┐ ┌──┴────┐ ┌┴───────┐ ┌──────┴─────┐
    │ DO-254  │ │  CEH  │ │Customer│ │  Internal  │
    │         │ │ Issue │ │Expecta-│ │ Processes  │
    │         │ │ Paper │ │ tions  │ │            │
    └─────────┘ └───────┘ └────────┘ └────────────┘
```

- Company procedures contain guidance and templates for generating CEH documentation, PHAC, CIA and HAS

- In ever-changing environment, new initiatives upgrade company documentation procedures.

- **DER Expectation: Documentation that substantiates prudent engineering and demonstrates appropriate design assurance IAW AC 20-152**

Rockwell Collins

Current State – Review Matrix Example

10.1	Hardware Plans		
10.1.1	PHAC	(S) thru D	PHAC
10.1.1.1	System Overview		Design Plan, CEH DOC's
10.1.1.2	Hardware Overview		Design Plan, CEH DOC's
10.1.1.3	Certification Considerations		Design Plan, **CIA, PHAC**
10.1.1.4	Hardware Design Life Cycle		Design Plan
10.1.1.5	Hardware Design Life Cycle Data		Design Plan
10.1.1.6	Additional Considerations		Design Plan, **CIA, PHAC**
10.1.1.7	Alternative Methods		Design Plan, **CIA, PHAC**
10.1.1.8	Certification Schedule		Design Plan, **CIA, PHAC**

Rockwell Collins

Best Practices

- **Get Involved Early**

- **Be Clear and Simple About Expectations**

- **Provide Guidance, Examples and Templates**

- **Coach and mentor, but be tenacious**

- **Retain objectivity (2 hats)**

- **Encourage and support institutional change**

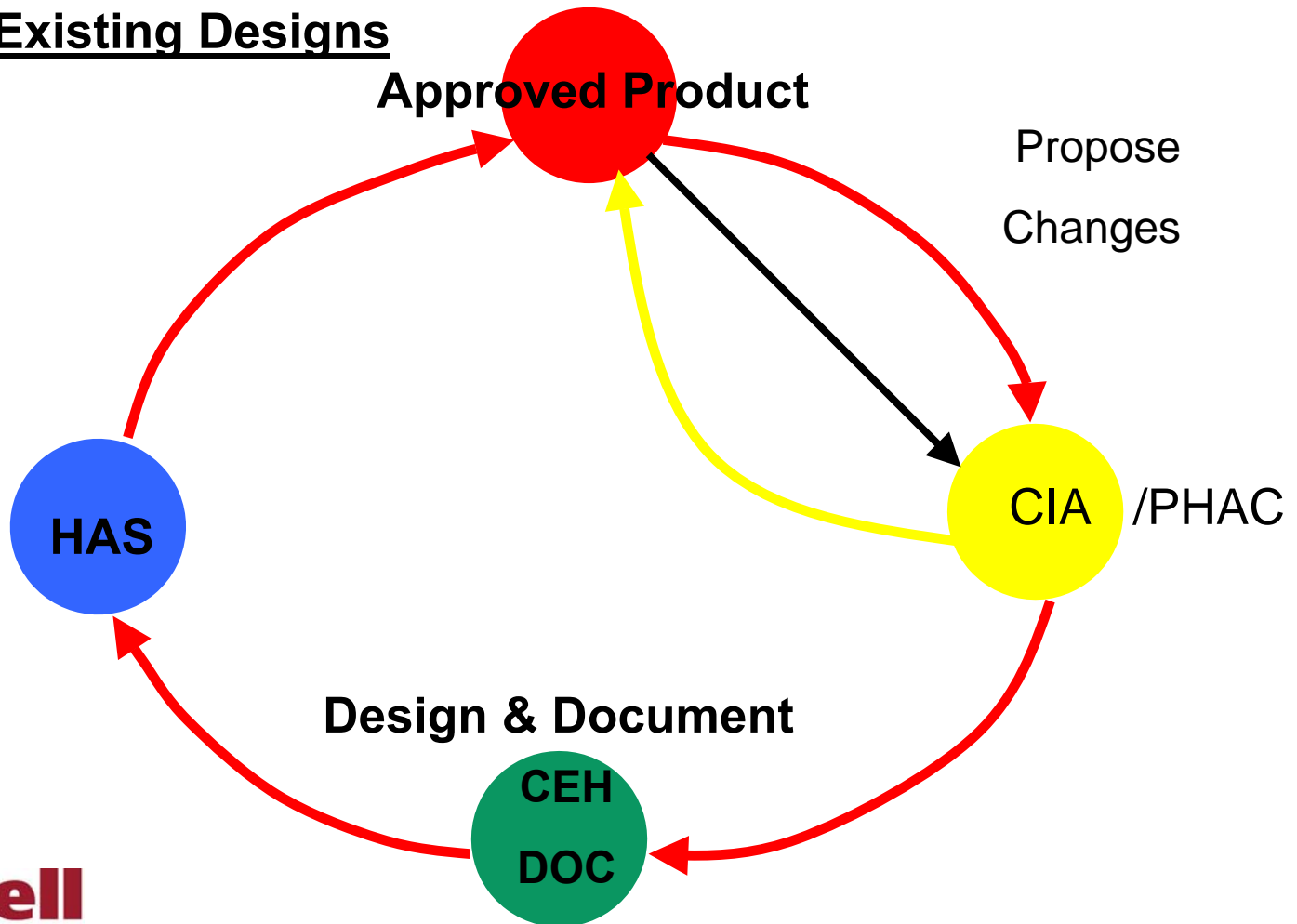- **In the end, ensure that compliance is properly documented.**

Rockwell Collins

Best Practices (cont.)

- **Get Involved Early in product development and ASIC design**

Product Development Cycle
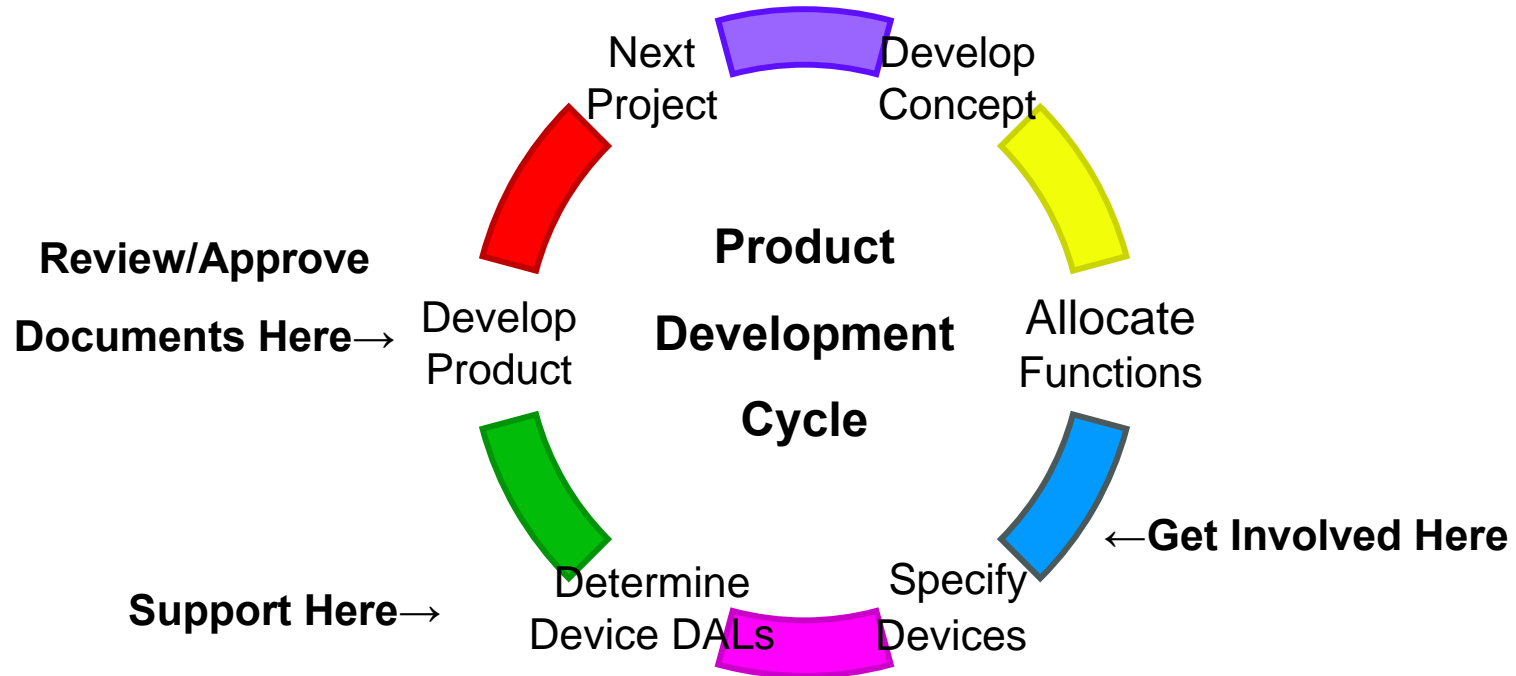
- Develop Concept
- Allocate Functions
- Specify Devices ←**Get Involved Here**
- Determine Device DALs — **Support Here→**
- Develop Product — **Review/Approve Documents Here→**
- Next Project

Modifying Existing Designs

Approved Product

Propose
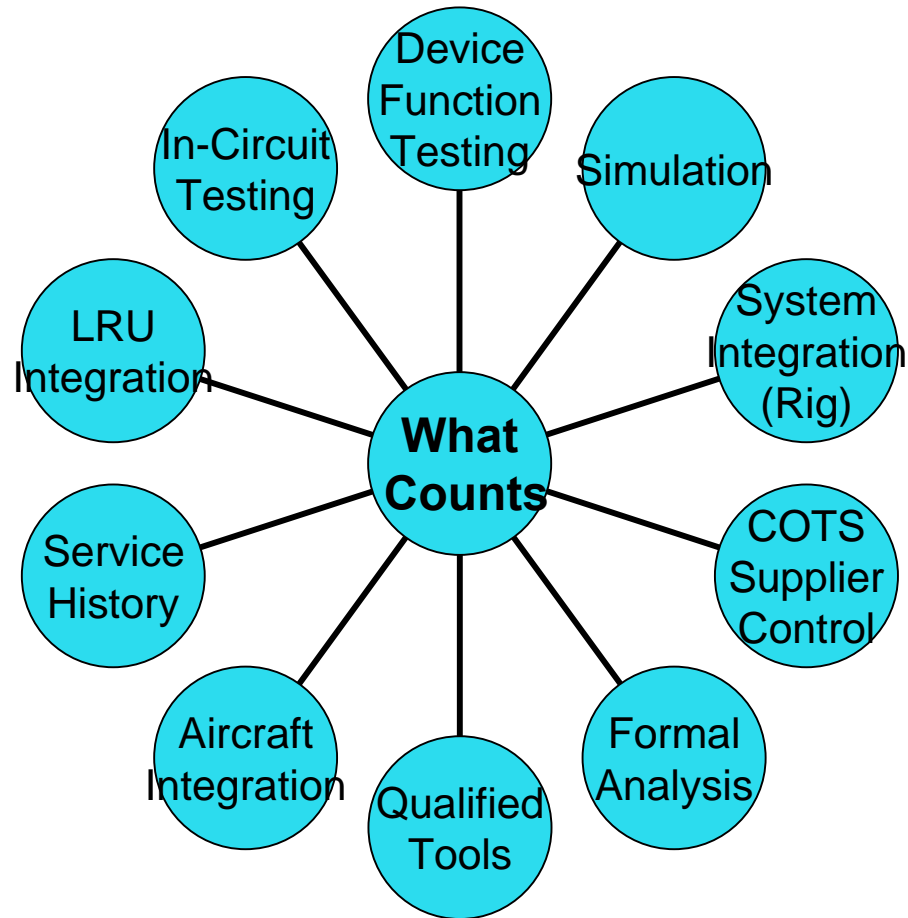
Changes

HAS

CIA /PHAC

Design & Document

CEH
DOC

- **Be Clear and Simple About Expectations**

    — **Documentation for DAL of CEH is required**

    — **New Products require PHAC**

    — **For existing products CIA might suffice – propose if change is minor**

    — **Supporting documentation should be stored in a controlled archive system**

    — **CIA/PHAC and HAS are deliverable as part of TSO package**

    — **Supporting documentation will often be reviewed by DER**

Rockwell Collins

Best Practices (cont.)

- **Provide Guidance, Examples and Templates**

  — **Trained to design; tend to resist "paperwork"**

  — **Want a successful delivery; will do what it takes**

  — **Prefer examples: it "shows" what you want**

  — **Templates with narrative description:**

    — **are useful for engineers to speed documentation**

    — **Allow better standardization of content and its location**

Rockwell Collins

A diagram centered on "What Counts" with connected nodes: Device Function Testing, Simulation, In-Circuit Testing, System Integration (Rig), LRU Integration, COTS Supplier Control, Service History, Formal Analysis, Aircraft Integration, Qualified Tools.

Best Practices (cont.)

- **Coach**
  - — **Help them to find ways within their structure to economize**

- **Mentor**
  - — **Help them to become mostly autonomous**

- **Be Tenacious**
  - — **Let it be a learning exercise, not a battle of wills**

Rockwell Collins

Best Practices (cont.)

- **Retain Objectivity**

  - **Company Hat**

    - **Technical Expertise**

    - **Design Process Familiarity**

    FAA DER Hat

    - **Regulatory Expertise**

    - **Certification Process Familiarity**

Best Practices (cont.)

- **Encourage and Support Institutional Change**

  — **AC 20-152 Is Published!**

  — **Communicate benefits to engineering management**

  — **Propose improvements to current means of documenting assurance**

  — **Identify areas of reuse**

  — **Throughout - Patience**

Best Practices (cont.)

- **Ensure Compliance Documentation is on Target**

    — **What is the functionality?**

    — **How is it implemented?**

    — **Is the appropriate DAL been identified?**

    — **How is design assurance demonstrated?**

    — **Do the verification results show satisfaction of the requirements and DAL?**

- **BOTTOM LINE: COMPLIANT?**

Future – What We Anticipate

- **An FAA Order (similar to 8110.49) for CEH**

- **An FAA Policy Memo?**

- **TSO incorporation through Order 8150.1c?**

- **Reduction (or elimination) of emphasis on Issue Papers and additional customer expectations**

- **Consolidation of resources with focus on proper interpretation and implementation of AC 20-152, as well as appropriate use of guidance and procedures in DO-254**

Rockwell Collins

Conclusions

- **AC 20-152 provides solid framework and focus for engineering and assurance documentation efforts.**

- **We can now assess and make meaningful improvements with confidence.**

- **Accepted best practices within any organization will most likely include finding ways to use existing approaches as much as possible**

- **The expectation remains that the designers will provide documentation of prudent engineering, thereby showing compliance.**

Rockwell Collins